maker subject to prosecution under 18 U.S.C. 1001.

(End of provision)

1252.237–72 Prohibition on advertising.

As prescribed in (TAR) 48 CFR 1213.7101 and 1237.7003, insert the following clause:

PROHIBITION ON ADVERTISING (JAN 1996)

The contractor or its representatives (including training instructors) shall not advertise or solicit business from attendees for private, non-Government training during contracted-for training sessions. This prohibition extends to unsolicited oral comments, distribution or sales of written materials, and/or sales of promotional videos or audio tapes. The contractor agrees to insert this clause in its subcontracts.

(End of clause)

1252.237–73 Key personnel.

As prescribed in (TAR) 48 CFR 1237.110(b), insert the following clause:

KEY PERSONNEL (APR 2005)

(a) The personnel as specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel, as appropriate.

(b) Before removing, replacing, or diverting any of the specified individuals, the Contractor shall notify the contracting officer, in writing, before the change becomes effective. The Contractor shall submit information to support the proposed action to enable the contracting officer to evaluate the potential impact of the change on the contract. The Contractor shall not remove or replace personnel under this contract until the Contracting Officer approves the change.

The Key Personnel under this Contract are: (*specify key personnel*)

(End of clause)

1252.239–70 Security requirements for unclassified information technology resources.

As prescribed in (TAR) 48 CFR 1239.70, insert the following clause:

SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (APR 2005)

(a) The Contractor shall be responsible for Information Technology security for all systems connected to a Department of Transportation (DOT) network or operated by the Contractor for DOT, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the Contractor has physical or electronic access to DOT's sensitive information that directly supports the mission of DOT. The term ''information technology,'' as used in this clause, means any equipment or interconnected system or subsystem of equipment, including telecommunications equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes both major applications and general support systems as defined by OMB Circular A–130. Examples of tasks that require security provisions include:

(1) Hosting of DOT e-Government sites or other IT operations;

(2) Acquisition, transmission or analysis of data owned by DOT with significant replacement cost should the contractor's copy be corrupted; and

(3) Access to DOT general support systems/major applications at a level beyond that granted the general public, e.g. bypassing a firewall.

(b) The Contractor shall develop, provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. The plan shall describe those parts of the contract to which this clause applies. The Contractor's IT Security Plan shall comply with applicable Federal Laws that include, but are not limited to, 40 U.S.C. 11331, the Federal Information Security Management Act (FISMA) of 2002 and the E-Government Act of 2002. The plan shall meet IT security requirements in accordance with Federal and DOT policies and procedures, as they may be amended from time to time during the term of this contract that include, but are not limited to:

(1) OMB Circular A–130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources;

(2) National Institute of Standards and Technology (NIST) Guidelines;

(3) Departmental Information Resource Management Manual (DIRMM) and associated guidelines; and

(4) DOT Order 1630.2B, Personnel Security Management

(c) Within 30 days after contract award, the contractor shall submit the IT Security Plan to the DOT Contracting Officer for acceptance. This plan shall be consistent with and further detail the approach contained in